

ON THE BERNOULLI AUTOMORPHISM OF REVERSIBLE LINEAR CELLULAR AUTOMATA

CHIH-HUNG CHANG AND HUILAN CHANG

ABSTRACT. This investigation studies the ergodic properties of reversible linear cellular automata over \mathbb{Z}_m for $m \in \mathbb{N}$. We show that a reversible linear cellular automaton is either a Bernoulli automorphism or non-ergodic. This gives an affirmative answer to an open problem proposed in [Pivato, Ergodic theory of cellular automata, Encyclopedia of Complexity and Systems Science, 2009, pp. 2980-3015] for the case of reversible linear cellular automata.

1. INTRODUCTION

Motivated by biological applications, John von Neumann introduced cellular automata (CAs) in the late 1940s. The main goal was to design self-replicating artificial systems that are also computationally universal and are analogous to human brain. Namely, CA is designed as a computing device in which the memory and the processing units are not separated from each other, and is massively parallel and capable of repairing and building itself given the necessary raw material.

CA has been systematically studied by Hedlund from purely mathematical point of view [9]. For the past few decades, studying CA from the viewpoint of the ergodic theory has received remarkable attention [1, 2, 5, 6, 10, 14, 21, 22]. Pivato has characterized the invariant measures of bipermutative right-sided, nearest neighbor cellular automata [19]. Moreover,

Date: September 21, 2015.

1991 Mathematics Subject Classification. Primary 37A05; Secondary 37B15, 28D20.

Key words and phrases. Measure-preserving transformation, invertible cellular automata, strong mixing, Bernoulli automorphism.

This work is partially supported by the Ministry of Science and Technology, ROC (Contract No MOST 103-2115-M-390-002- and 103-2115-M-390-004-).

Pivato and Yassawi introduced the concepts of harmonic mixing for measures and diffusion for a linear CA and developed broad sufficient conditions for convergence the limit measures [21, 22]. Sablik demonstrates the measure rigidity and directional dynamics for CA [23, 24]. Host *et al.* have studied the role of uniform Bernoulli measure in the dynamics of cellular automata of algebraic origin [10]. Furthermore, the sufficient conditions whether a one-dimensional permutative CA is strong mixing, k -mixing, or Bernoulli automorphic were independently revealed by Klevland and Shereshevsky [14, 25, 26]. Recently, one-sided expansive invertible cellular automata and two-sided expansive permutation cellular automata have been demonstrated to be strong mixing (see [3, 4, 12, 13, 17]).

Almost all the results about are for one-dimensional (mostly permutative) CA and for the uniform measure. It is natural to ask the following question:

Problem 1 (See [20]). Can mixing and ergodicity be obtained for non-permutative CA and/or non-uniform measures? What about multidimensional CA?

Theorem 2.5 and Corollary 2.4 indicate that an invertible linear CA is either Bernoulli automorphic or non-ergodic for the uniform Bernoulli measure. In [6], Cattaneo *et al.* address a necessary and sufficient condition for the ergodicity of linear CA. Corollary 2.4 reveals a concise condition for the ergodicity of invertible CA. The result remains true for those measures satisfying some conditions (see Remark 6.1). The methodology can be extended to the investigation of multidimensional invertible linear CA, and even possible to the non-permutative cases. Related works are under preparation.

The rest of this paper is organized as follows. Section 2 states the main results and some preliminaries. The proofs are postponed to Sections 4 and 5 while the key ideas are revealed via some examples in Section 3. Discussion and further works are addressed in Section 6.

2. STATEMENT OF MAIN RESULTS

Let $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ be the ring of the integers modulo m , where $m \geq 2$, and let $\mathbb{Z}_m^{\mathbb{Z}}$ be the space of all doubly-infinite sequences $x = (x_n)_{n=-\infty}^{\infty} \in \mathbb{Z}_m^{\mathbb{Z}}$, equipped with the product of the Tychonoff topology. Then the shift $\sigma : \mathbb{Z}_m^{\mathbb{Z}} \rightarrow \mathbb{Z}_m^{\mathbb{Z}}$ defined by $(\sigma x)_i = x_{i+1}$ is a homeomorphism of the compact metric space $\mathbb{Z}_m^{\mathbb{Z}}$. A one-dimension cellular automaton is a continuous map $T_f : \mathbb{Z}_m^{\mathbb{Z}} \rightarrow \mathbb{Z}_m^{\mathbb{Z}}$ defined by $(T_f x)_i = f(x_{i+l}, \dots, x_{i+r})$, where $l, r \in \mathbb{Z}$ and $f : \mathbb{Z}_m^{r-l+1} \rightarrow \mathbb{Z}_m$ is a given local rule or map. A local rule f is said to be linear if it can be written as

$$f(x_l, \dots, x_r) = \sum_{i=l}^r \lambda_i x_i \pmod{m}, \quad l, r \in \mathbb{Z},$$

where at least one among $\lambda_l, \dots, \lambda_r$ is nonzero in \mathbb{Z}_m [8, 16].

A local rule f is said to be permutative in x_j (or, at the index j) if for any given finite sequence

$$(\bar{x}_l, \dots, \bar{x}_{j-1}, \bar{x}_{j+1}, \dots, \bar{x}_r) \in \mathbb{Z}_m^{r-l}$$

we have

$$\{f(\bar{x}_l, \dots, \bar{x}_{j-1}, x_j, \bar{x}_{j+1}, \dots, \bar{x}_r) : x_j \in \mathbb{Z}_m\} = \mathbb{Z}_m.$$

The notion of permutative cellular automata was first introduced by Hedlund [9]. A linear local rule f is permutative at the index j if and only if $\gcd(\lambda_j, m) = 1$, where $\gcd(p, q)$ denotes the greatest common divisor of p and q .

For every linear local rule $f(x_l, \dots, x_r) = \sum_{i=l}^r \lambda_i x_i \pmod{m}$, there associates a formal power series $F(X) = \sum_{i=l}^r \lambda_i X^{-i}$. Let T_f be the cellular automaton defined by the local rule f . Ito et al. characterize the necessary and sufficient condition for the invertibility of T_f .

Theorem 2.1 (See [11]). *T_f is invertible if and only if for each prime factor $p|m$ there exists a unique j_p such that f is permutative at the index j_p .*

For the case where $m = p^k$ for some prime number p and $k \in \mathbb{N}$, it comes immediately that T_f is invertible if and only if there exists a unique j such

that $\gcd(\lambda_j, p) = 1$. Manzini and Margara demonstrate the corresponding formal power series $F(X)$ is invertible in $\mathbb{Z}_m[[X, X^{-1}]]$.

Theorem 2.2 (See [15]). *Suppose $m = p^k$ and T_f is invertible. Write $F(X) = \lambda_{j_p} X^{-j_p} + pH(X)$. Let $\tilde{H}(X) = -\lambda_{j_p} X^{j_p} H(X)$. Then*

$$F^{-1}(X) = \lambda_{j_p}^{-1} X^{j_p} (1 + p\tilde{H}(X) + \cdots + p^{k-1} \tilde{H}^{k-1}(X)),$$

where $\lambda_{j_p}^{-1}$ is the inverse element of λ_{j_p} in \mathbb{Z}_m .

Let $T : X \rightarrow X$ be a measure-preserving transformation on a probability space (X, \mathcal{B}, μ) . T is called *strong mixing* if

$$\lim_{n \rightarrow \infty} \mu(T^{-n} A \cap B) = \mu(A)\mu(B)$$

for any $A, B \in \mathcal{B}$. Furthermore, T is called *k-mixing* if for every given $\{A_i\}_{i=0}^k \subset \mathcal{B}$,

$$\lim_{n_1, n_2, \dots, n_k \rightarrow \infty} \mu(A_0 \cap T^{-n_1} A_1 \cap \cdots \cap T^{-(n_1 + \cdots + n_k)} A_k) = \mu(A_0)\mu(A_1) \cdots \mu(A_k).$$

It is seen that strong mixing is 1-mixing.

It is known that every surjective cellular automaton preserves the uniform Bernoulli measure (cf. [7, 14, 25] for instance). For the rest of this paper, μ refers to the uniform Bernoulli measure unless stated otherwise. Kleveland [14] and Shereshevsky [25, 26] have proved that T_f is strong mixing if $r < 0$ (resp. $l > 0$) and f is left permutative (resp. right permutative); some of these cellular automata are even *k-mixing*. Recently, one-sided expansive invertible cellular automata and two-sided expansive permutation cellular automata have been demonstrated to be strong mixing (see [3, 4, 12, 13, 17]). Theorem 2.3 addresses the necessary and sufficient condition for whether an invertible linear cellular automaton is strong mixing, which is an extension and characterizes the strong mixing property of invertible linear cellular automata completely.

Theorem 2.3. *An invertible linear cellular automaton T_f is strong mixing with respect to the uniform Bernoulli measure if and only if $j_p \neq 0$ for every prime factor p of m .*

The following corollary, which can be derived from the demonstration of Theorem 2.3 with a minor modification, addresses the “opposite” result to the above theorem. Notably, a one-dimensional linear cellular automaton with local rule $f(x_{-r}, \dots, x_r) = \sum_{i=-1}^r \lambda_i x_i \pmod{m}$ is ergodic if and only if $\gcd(\lambda_{-r}, \dots, \lambda_{-1}, \lambda_1, \dots, \lambda_r, m) = 1$ [6]. (In fact, a necessary and sufficient condition for the ergodicity of a multidimensional linear cellular automaton is demonstrated in [6].) Corollary 2.4 indicates a concise if-and-only-if condition for the ergodicity of one-dimensional invertible linear cellular automaton.

Corollary 2.4. *An invertible linear cellular automaton T_f is non-ergodic with respect to the uniform Bernoulli measure if and only if $j_p = 0$ for some prime factor p of m .*

Recall that T is ergodic if and only if $\lim_{n \rightarrow \infty} \mu(T^{-n}A \cap B) > 0$ for any $A, B \in \mathcal{B}$ with positive measures. Examples 3.1 and 3.2 interpret an intuitive idea for the reliability of Theorem 2.3; the rigorous proof is postponed to Section 4.

A stronger property in ergodic theory is *Bernoulli automorphism*. Given $\epsilon \geq 0$, two partitions $\xi = \{C_i\}$ and $\eta = \{D_j\}$ of the measure space $(\mathbb{Z}_m^{\mathbb{Z}}, \mathcal{B}, \mu)$ are said to be ϵ -independent if

$$\sum_{i,j} |\mu(C_i \cap D_j) - \mu(C_i)\mu(D_j)| \leq \epsilon.$$

ξ and η are independent if $\epsilon = 0$. A partition $\xi = \{C_i\}$ is called *Bernoulli* for an automorphism T_f if there exists an integer $N > 0$ such that the partitions $\bigvee_{k=-n}^0 T^k \xi$ and $\bigvee_{k=N}^{N+n} T^k \xi$ are independent for all $n \geq 0$. Furthermore, T_f is a Bernoulli automorphism if T_f has a generating Bernoulli partition.

Suppose the local rule f is permutative in the variable x_r (resp. x_l) and $0 \leq l < r$ (resp. $l < r \leq 0$), Shereshevsky showed that the natural extension of the dynamical system $(\mathbb{Z}_m^{\mathbb{Z}}, \mathcal{B}, \mu, T_f)$ is a Bernoulli automorphism [25, 26]. It is well-known that a Bernoulli automorphism is also strong mixing. With

the similar discussion of the demonstration of Theorem 2.3, we extend the results to the class of invertible linear cellular automata.

Theorem 2.5. *An invertible linear cellular automaton T_f is a Bernoulli automorphism with respect to the uniform Bernoulli measure if and only if $j_p \neq 0$ for every prime factor p of m .*

3. EXAMPLES

This section clarifies the key ideas of the proof of Theorems 2.3 and 2.5 and Corollary 2.4 by examining three examples.

Example 3.1. Consider $m = 4 = 2^2$ and $f(x_1, x_2, x_3) = 2x_1 + x_2 + 2x_3 \pmod{4}$. It follows that $f^{-1}(x_{-3}, x_{-2}, x_{-1}) = 2x_{-3} + x_{-2} + 2x_{-1} \pmod{4}$, and

$$f^{2n}(x_{4n}) = x_{4n} \pmod{4}, \quad f^{-2n}(x_{-4n}) = x_{-4n} \pmod{4}.$$

Given any other cylinder $[a_{L'}, \dots, a_{R'}]_{L'}^{R'}$, there exists $N \in \mathbb{N}$ such that $R' < L + 4n$ for $n \geq N$. It is well-known that all surjective CA preserve the uniform Bernoulli measure μ . Therefore,

$$\begin{aligned} & \mu(T_f^{-k}[a_L, \dots, a_R]_L^R \cap [a_{L'}, \dots, a_{R'}]_{L'}^{R'}) \\ &= \mu(T_f^{-k}[a_L, \dots, a_R]_L^R) \mu([a_{L'}, \dots, a_{R'}]_{L'}^{R'}) \\ &= \mu([a_L, \dots, a_R]_L^R) \mu([a_{L'}, \dots, a_{R'}]_{L'}^{R'}) \end{aligned}$$

for $k \geq 2N$. This demonstrates T_f is strong mixing.

Next example investigates the case where m has two distinct prime factors. The discussion can be extended to more general cases.

Example 3.2. Suppose $m = 12 = 2^2 \cdot 3$ and $f(x_0, x_1, x_2) = 6x_0 + 3x_1 + 2x_2 \pmod{12}$. Let ϕ_4 and ϕ_3 be the canonical projections from \mathbb{Z}_{12} to \mathbb{Z}_4 and \mathbb{Z}_3 , respectively. Then $\Phi := \Phi_4 \times \Phi_3$ is an isomorphism from $\mathbb{Z}_{12}^{\mathbb{Z}}$ to $\mathbb{Z}_4^{\mathbb{Z}} \times \mathbb{Z}_3^{\mathbb{Z}}$, where $\Phi_4 : \mathbb{Z}_{12}^{\mathbb{Z}} \rightarrow \mathbb{Z}_4^{\mathbb{Z}}$ and $\Phi_3 : \mathbb{Z}_{12}^{\mathbb{Z}} \rightarrow \mathbb{Z}_3^{\mathbb{Z}}$ are obtained from ϕ_4 and ϕ_3 , respectively.

Let f_4 and f_3 be defined as

$$f_4(x_0, x_1, x_2) = f(x_0, x_1, x_2) \pmod{4}$$

and

$$f_3(x_0, x_1, x_2) = f(x_0, x_1, x_2) \pmod{3},$$

respectively. In other words,

$$f_4(x_0, x_1, x_2) = 2x_0 + 3x_1 + 2x_2 \pmod{4},$$

$$f_3(x_0, x_1, x_2) = 2x_2 \pmod{3}.$$

Then the projections of T_f on $\mathbb{Z}_4^{\mathbb{Z}}$ and $\mathbb{Z}_3^{\mathbb{Z}}$, denoted by T_4 and T_3 , are the cellular automata with local rules f_4 and f_3 , respectively. Furthermore, let μ_4 and μ_3 be the push-forward measures of Φ_4 and Φ_3 , respectively. μ is the uniform Bernoulli measure on $\mathbb{Z}_{12}^{\mathbb{Z}}$ indicates that

- 1) μ_4 and μ_3 are the uniform Bernoulli measures on $\mathbb{Z}_4^{\mathbb{Z}}$ and $\mathbb{Z}_3^{\mathbb{Z}}$, respectively.
- 2) $\mu \cong \mu_4 \times \mu_3$.
- 3) $T_f \cong T_4 \times T_3$, and the diagram

$$\begin{array}{ccc} \mathbb{Z}_{12}^{\mathbb{Z}} & \xrightarrow{T_f} & \mathbb{Z}_{12}^{\mathbb{Z}} \\ \Phi \downarrow & & \downarrow \Phi \\ \mathbb{Z}_4^{\mathbb{Z}} \times \mathbb{Z}_3^{\mathbb{Z}} & \xrightarrow{T_4 \times T_3} & \mathbb{Z}_4^{\mathbb{Z}} \times \mathbb{Z}_3^{\mathbb{Z}} \end{array}$$

is commutative.

Similar to the discussion of Example 3.1, the local rule of T_4^{-1} is expressed as

$$f_4^{-1}(x_{-2}, x_{-1}, x_0) = 2x_{-2} + 3x_{-1} + 2x_0 \pmod{4},$$

and

$$f_4^{2n}(x_{2n}) = x_{2n} \pmod{4}, \quad f_4^{-2n}(x_{-2n}) = x_{-2n} \pmod{4}$$

Given any other cylinder $U' = [a_{L'}, \dots, a_{R'}]_{L'}^{R'}$, pick $N = \lfloor \frac{|R'-L|}{2} \rfloor + 1$. It follows immediately

$$(1) \quad \mu_4(T_4^{-k}U_4 \cap U'_4) = \mu_4(T_4^{-k}U_4)\mu_4(U'_4) = \mu_4(U_4)\mu_4(U'_4) \quad \text{for } k \geq 2N$$

since $L + k > R'$, where $A_j := \Phi_j(A)$ for $A \in \mathcal{B}$.

Similarly, the local rule of T_3^{-1} is $f_3^{-1}(x_{-2}) = 2x_{-2} \pmod{3}$. This infers

$$f_3^{-n} = \begin{cases} 2x_{-2n}, & n \text{ is odd;} \\ x_{-2n}, & n \text{ is even.} \end{cases}$$

It is seen that $\mu_3(T_3^{-n}U_3) = \mu_3(U_3)$ for all n and

$$(2) \quad \mu_3(T_3^{-k}U_3 \cap U'_3) = \mu_3(T_3^{-k}U_3)\mu_3(U'_3) = \mu_3(U_3)\mu_3(U'_3) \quad \text{for } k \geq N.$$

Combining (1) and (2) we have, for $k \geq 2N$,

$$\begin{aligned} \mu(T_f^{-k}U \cap U') &= (\mu_4 \times \mu_3)[(T^{-k}U \cap U')_4 \times (T^{-k}U \cap U')_3] \\ &= \mu_4((T^{-k}U \cap U')_4)\mu_3((T^{-k}U \cap U')_3) \\ &= \mu_4(T_4^{-k}U_4 \cap U'_4)\mu_3(T_3^{-k}U_3 \cap U'_3) \\ &= (\mu_4 \times \mu_3)(U_4 \times U_3) \cdot (\mu_4 \times \mu_3)(U'_4 \times U'_3) = \mu(U)\mu(U'). \end{aligned}$$

The strong mixing property of T_f then follows.

Next example addresses that T_f is even non-ergodic if $j_p = 0$ for some $p|m$.

Example 3.3. Let $m = 36 = 2^2 \cdot 3^2$ and let f be given as

$$f(x_{-1}, x_0, x_1) = 15x_{-1} + 10x_0 + 6x_1 \pmod{36}.$$

It is seen that $j_2 = -1$ and $j_3 = 0$. To deduce that T_f is not ergodic, we firstly observe that

$$f^{6k} = 9x_{-6k} + 28x_0 \pmod{36} \quad \text{and} \quad f^{-6k} = 28x_0 + 9x_{6k} \pmod{36}$$

for all $k \in \mathbb{N}$. Suppose $U = [0]_0$. Then α_0 is a multiple of 9 for each $\alpha = (\alpha_i) \in T_f^{-6k}(U)$. Hence T_f is not ergodic since $T_f^{-6k}(U) \cap [1]_0 = \emptyset$ for all k .

4. PROOF OF THEOREM 2.3

This section is devoted to demonstrating an invertible linear cellular automaton is strong mixing if and only if $j_p \neq 0$ for all prime factor p of the integer m . One can verify without difficulty that the existence of prime factor p of m such that $j_p = 0$ infers such a cellular automaton is not ergodic,

thus it is not strong mixing. (An intuitive exploration is that $j_p = 0$ for some prime factor p indicates T_p^n is a trivial shift map for some $n \in \mathbb{N}$, where $T_p \equiv T \pmod{p^k}$ and $p^k | m, p^{k+1} \nmid m$.) It remains to show the “if” part of Theorem 2.3.

Let \mathcal{L} be the collection of linear local rules and let

$$\mathbb{Z}_m[X, X^{-1}] = \{\sum_{i=l}^r a_i x^i, l, r \in \mathbb{Z}\}$$

be the set of bi-polynomials of variable X . Define a mapping $\chi : \mathcal{L} \rightarrow \mathbb{Z}_m[X, X^{-1}]$, which relates a linear local rule f to a bi-polynomial $F(X)$, as

$$\chi(f) = \chi(\sum_{i=l}^r \lambda_i x_i) = \sum_{i=l}^r \lambda_i X^{-i} := F(X).$$

It is easily seen that χ is bijective. Moreover, let $\mathbb{Z}_m[[X, X^{-1}]]$ denote the formal power series generated by $\{X, X^{-1}\}$ over \mathbb{Z}_m . Then $\widehat{\chi} : \mathbb{Z}_m^{\mathbb{Z}} \rightarrow \mathbb{Z}_m[[X, X^{-1}]]$ defined by

$$\widehat{\chi}(\mathbf{b}) = \sum_{i=-\infty}^{\infty} b_i X^i, \quad \text{where } \mathbf{b} = (b_i)_{i \in \mathbb{Z}} \in \mathbb{Z}_m^{\mathbb{Z}}$$

is also a bijection. Observe that, for each $\mathbf{b} = (b_i) \in \mathbb{Z}_m^{\mathbb{Z}}$,

$$\widehat{\chi}(T_f(\mathbf{b})) = \widehat{\chi}\left(\left(\sum_{n=l+i}^{r+i} \lambda_{n-i} b_n\right)_i\right) = \sum_{i=-\infty}^{\infty} \left(\sum_{n=l+i}^{r+i} \lambda_{n-i} b_n\right) X^i,$$

and

$$\begin{aligned} \mathbb{T}(\widehat{\chi}(\mathbf{b})) &= \mathbb{T}\left(\sum_{i=-\infty}^{\infty} b_i X^i\right) \\ &= \left(\sum_{n=l}^r \lambda_n X^{-n}\right) \left(\sum_{i=-\infty}^{\infty} b_i X^i\right) = \sum_{i=-\infty}^{\infty} \left(\sum_{n=l+i}^{r+i} \lambda_{n-i} b_n\right) X^i, \end{aligned}$$

where $\mathbb{T}(\Theta(X)) := F(X)\Theta(X)$. This implements that the diagram

$$(3) \quad \begin{array}{ccc} \mathbb{Z}_m^{\mathbb{Z}} & \xrightarrow{T} & \mathbb{Z}_m^{\mathbb{Z}} \\ \widehat{\chi} \downarrow & & \downarrow \widehat{\chi} \\ \mathbb{Z}_m[[X, X^{-1}]] & \xrightarrow{\mathbb{T}} & \mathbb{Z}_m[[X, X^{-1}]] \end{array}$$

commutes. Moreover, it follows immediately from the mathematical induction that $f^n = \chi^{-1}((F(X))^n)$ for all $n \in \mathbb{N}$, where $f^n = f \circ f^{n-1}$.

Suppose $m = p^k$ for some prime number p and $k \in \mathbb{N}$. Write $F(X)$ as $F(X) = \lambda_{j_p} X^{-j_p} + pH(X)$.

Lemma 4.1. $(F(X))^{p^{k-1}} \equiv \lambda_{j_p}^m X^{-p^{(k-1)}j_p} \pmod{p^k}$.

Proof. Observe that

$$\begin{aligned}
(\lambda_{j_p} X^{-j_p} + pH(X))^p &= \sum_{j=0}^p \binom{p}{j} (\lambda_{j_p} X^{-j_p})^j (pH(X))^{p-j} \\
&\equiv \sum_{j=p-1}^p \binom{p}{j} (\lambda_{j_p} X^{-j_p})^j (pH(X))^{p-j} \pmod{p^2} \\
&= p(\lambda_{j_p} X^{-j_p})^{p-1} (pH(X)) + (\lambda_{j_p} X^{-j_p})^p \\
&\equiv \lambda_{j_p}^p X^{-pj_p} \pmod{p^2}
\end{aligned}$$

Given $n \in \mathbb{N}$, let

$$\phi(n) = \#\{i : 1 \leq i \leq n, \gcd(i, n) = 1\}$$

be *Euler's totient function*. Euler indicated that

$$a^{\phi(n)} \equiv 1 \pmod{n} \quad \text{for all } \gcd(a, n) = 1.$$

More specifically, $a^{p^{k-1}} \equiv a^{p^k} \pmod{p^k}$ for all $\gcd(a, p) = 1$. This implies

$$(\lambda_{j_p} X^{-j_p} + pH(X))^p \equiv \lambda_{j_p}^{p^2} X^{-pj_p} \pmod{p^2}$$

Assume that Lemma 4.1 holds for $m = p^{k-1}$, that is,

$$(F(X))^{p^{k-2}} = p^{k-1}Q(X) + \lambda_{j_p}^{p^{k-2}} X^{-p^{(k-2)}j_p}$$

for some $Q(X)$. Therefore,

$$\begin{aligned}
(F(X))^{p^{k-1}} &= \left(p^{k-1}Q(X) + \lambda_{j_p}^{p^{k-2}} X^{-p^{(k-2)}j_p} \right)^p \\
&= \sum_{j=0}^p \binom{p}{j} (p^{k-1}Q(X))^j \left(\lambda_{j_p}^{p^{k-2}} X^{-p^{(k-2)}j_p} \right)^{p-j} \\
&\equiv \sum_{j=0}^1 \binom{p}{j} (p^{k-1}Q(X))^j \left(\lambda_{j_p}^{p^{k-2}} X^{-p^{(k-2)}j_p} \right)^{p-j} \pmod{p^k} \\
&\equiv \lambda_{j_p}^{p^{k-1}} X^{-p^{(k-1)}j_p} \pmod{p^k} \\
&\equiv \lambda_{j_p}^{p^k} X^{-p^{(k-1)}j_p} \pmod{p^k}
\end{aligned}$$

This completes the proof. \square

Suppose T_f is an invertible linear cellular automaton. Theorem 2.2 infers that T_f^{-1} is a linear cellular automaton with local rule $f^{-1} = \chi^{-1}(F^{-1}(X))$, where

$$F^{-1}(X) = \lambda_{j_p}^{-1} X^{j_p} (1 + p\tilde{H}(X) + \dots + p^{k-1}\tilde{H}^{k-1}(X))$$

and $\tilde{H}(X) = -\lambda_{j_p} X^{j_p} H(X)$. Since $F^{-1}(X)$ is also of the form $F^{-1}(X) = \lambda_{j_p}^{-1} X^{j_p} + p\overline{H}(X)$, it follows from Lemma 4.1 that

$$(4) \quad (F^{-1}(X))^{p^{k-1}} \equiv \lambda_{j_p}^{-m} X^{p^{k-1}j_p} \pmod{p^k}.$$

For the clarification of the discussion, the notation $g \leftrightarrow [t_1, t_2]$ refers to the local rule $g(x_{t_1}, \dots, x_{t_2}) = \sum_{i=t_1}^{t_2} \lambda_i x_i \pmod{m}$. Combining the one-to-one correspondence between \mathcal{L} and $\mathbb{Z}_m[X, X^{-1}]$, Lemma 4.1, and the commutative diagram (3), a straightforward examination deduces that

$$(5) \quad f^n \leftrightarrow [\ell p^{k-1} j_p], \quad f^{-n} \leftrightarrow [-\ell p^{k-1} j_p],$$

if $n = \ell p^{k-1}$ for some $\ell \in \mathbb{N}$, and

$$(6) \quad f^n \leftrightarrow [\ell p^{k-1} j_p + \ell' l, \ell p^{k-1} j_p + \ell' r],$$

$$(7) \quad f^{-n} \leftrightarrow [-\ell p^{k-1} j_p + \ell' \bar{l}, -\ell p^{k-1} j_p + \ell' \bar{r}],$$

if $n = \ell p^{k-1} + \ell'$ for some $\ell \in \mathbb{N}, 1 \leq \ell' < p^{k-1}$, where

$$\bar{l} = (l - j_p)(k-1) - j_p, \quad \bar{r} = (r - j_p)(k-1) - j_p.$$

The strong mixing property of invertible cellular automaton for the case where m is a multiple power of a prime number follows via (5), (6), and (7).

Lemma 4.2. *Suppose $m = p^k$ for some prime number p and $k \in \mathbb{N}$. Then an invertible linear cellular automaton is strong mixing if and only if $j_p \neq 0$.*

Proof. The “only if” part follows immediately from (5). Given any two cylinders $U, V \in \mathbb{Z}_m^{\mathbb{Z}}$, write U and V as $U = [U]_{u_l}^{u_r}$ and $V = [V]_{v_l}^{v_r}$, respectively, for some $u_l, u_r, v_l, v_r \in \mathbb{Z}$. Herein the notation $[\alpha]_{i_1}^{i_2}$, $i_1 \leq i_2$, refers to the cylinder

$$i_1[\alpha_{i_1}, \dots, \alpha_{i_2}]_{i_2} = \{x \in \mathbb{Z}_m^{\mathbb{Z}} : x_j = \alpha_j, i_1 \leq j \leq i_2\}.$$

Claim 4.3. $T_f^{-n}U$ is a finite union of cylinders for every $n \in \mathbb{Z}$.

To see this, it suffices to show the case where $n = 1$.

Obviously $T_f^{-1}U \subseteq [U']_{u'_l}^{u'_r}$, where

$$\begin{aligned} u'_l &= \min\{u_l - (l - j_p)(k - 1) + j_p, u_l - (r - j_p)(k - 1) + j_p\}, \\ u'_r &= \max\{u_r - (l - j_p)(k - 1) + j_p, u_r - (r - j_p)(k - 1) + j_p\}. \end{aligned}$$

$\gcd(\lambda_{j_p}^{-1}, m) \equiv 1 \pmod{m}$ indicates $f^{-1}(x_{l'}, \dots, x_{r'})$ is a permutation at x_{-j_p} , where $l' = (l - j_p)(k - 1) - j_p$, $r' = (r - j_p)(k - 1) - j_p$, and $l' \leq -j_p \leq r'$ or $r' \leq -j_p \leq l'$. A straightforward and careful verification deduces

$$(T_f^{-1}U)_i := \{x_i : x = (x_j) \in T_f^{-1}U\} = \mathbb{Z}_m$$

provided

$$i \in \mathbb{Z} \setminus \{\min\{u'_l, u'_r\}, \min\{u'_l, u'_r\} + 1, \dots, \max\{u'_l, u'_r\}\}.$$

In other words, $T_f^{-1}U$ is a finite union of cylinders, and Claim 4.3 follows.

Since $T_f^{-n}U$ is a finite union of cylinders, (5) and (7) imply that there exists $N \in \mathbb{N}$ such that $T_f^{-n}U \subseteq [U']_{u'_l}^{u'_r}$ satisfies either $u'_l > v_r$ or $u'_r < v_l$ for $n \geq N$. It follows that

$$\mu(T_f^{-n}U \cap V) = \mu(T_f^{-n}U)\mu(V) = \mu(U)\mu(V)$$

for $n \geq N$ since μ is T_f -invariant. This demonstrates the strong mixing property of invertible linear cellular automata for the case where $m = p^k$. \square

Notably, for every $n \in \mathbb{N}$ and cylinder U , neither $T_f^{-n}U$ nor T_f^nU are cylinders in general. It is seen in the proof of Lemma 4.2 that $T_f^{-1}U$ is a sub-cylinder of cylinder $[U']_{u'_l}^{u'_r}$ with $x_{u'_l}, \dots, x_{u'_r}$ being constrained by some equations came from f for all $x \in T_f^{-1}U$ (cf. Examples 3.1 and 3.2).

Suppose $m = sq$ for some coprime factors $s, q \in \mathbb{N}$. Define $f_s : \mathbb{Z}_s^{r-l+1} \rightarrow \mathbb{Z}_s$ and $f_q : \mathbb{Z}_q^{r-l+1} \rightarrow \mathbb{Z}_q$ by

$$f_s(x_l, \dots, x_r) = f(x_l, \dots, x_r) \pmod{s}$$

and

$$f_q(x_l, \dots, x_r) = f(x_l, \dots, x_r) \pmod{q},$$

respectively. Then f_s, f_q generate invertible cellular automata $T_s : \mathbb{Z}_s^{\mathbb{Z}} \rightarrow \mathbb{Z}_s^{\mathbb{Z}}$ and $T_q : \mathbb{Z}_q^{\mathbb{Z}} \rightarrow \mathbb{Z}_q^{\mathbb{Z}}$. Observe that the canonical isomorphism $\phi : \mathbb{Z}_m \rightarrow \mathbb{Z}_s \times \mathbb{Z}_q$ induces an isomorphism $\Phi : \mathbb{Z}_m^{\mathbb{Z}} \rightarrow \mathbb{Z}_s^{\mathbb{Z}} \times \mathbb{Z}_q^{\mathbb{Z}}$. A straightforward examination shows that the diagram

$$(8) \quad \begin{array}{ccc} \mathbb{Z}_m^{\mathbb{Z}} & \xrightarrow{T_f} & \mathbb{Z}_m^{\mathbb{Z}} \\ \Phi \downarrow & & \downarrow \Phi \\ \mathbb{Z}_s^{\mathbb{Z}} \times \mathbb{Z}_q^{\mathbb{Z}} & \xrightarrow{T_s \times T_q} & \mathbb{Z}_s^{\mathbb{Z}} \times \mathbb{Z}_q^{\mathbb{Z}} \end{array}$$

commutes.

Furthermore, let μ_s and μ_q be the push-forward measures of μ on $\mathbb{Z}_s^{\mathbb{Z}}$ and $\mathbb{Z}_q^{\mathbb{Z}}$ with respect to canonical projections Φ_s and Φ_q , respectively. It follows that $\mu \cong \mu_s \times \mu_q$. For any two measurable sets $U, V \in \mathbb{Z}_m^{\mathbb{Z}}$ such that

$$\mu_s(\Phi_s(U) \cap \Phi_s(V)) = \mu_s(\Phi_s(U)) \cdot \mu_s(\Phi_s(V))$$

and

$$\mu_q(\Phi_q(U) \cap \Phi_q(V)) = \mu_q(\Phi_q(U)) \cdot \mu_q(\Phi_q(V)),$$

one can see that

$$\begin{aligned} (\mu_s \times \mu_q)(\Phi(U \cap V)) &= \mu_s(\Phi_s(U \cap V)) \cdot \mu_q(\Phi_q(U \cap V)) \\ &= \mu_s(\Phi_s(U) \cap \Phi_s(V)) \cdot \mu_q(\Phi_q(U) \cap \Phi_q(V)) \\ &= [\mu_s(\Phi_s(U)) \cdot \mu_s(\Phi_s(V))] \cdot [\mu_q(\Phi_q(U)) \cdot \mu_q(\Phi_q(V))] \\ &= [\mu_s(\Phi_s(U)) \cdot \mu_q(\Phi_q(U))] \cdot [\mu_s(\Phi_s(V)) \cdot \mu_q(\Phi_q(V))] \\ &= (\mu_s \times \mu_q)(\Phi(U)) \cdot (\mu_s \times \mu_q)(\Phi(V)) = \mu(U) \cdot \mu(V). \end{aligned}$$

In other words,

$$(9) \quad \mu(U \cap V) = \mu(U) \cdot \mu(V).$$

For the general case, factorizing m into the product of its prime factors $m = p_1^{k_1} p_2^{k_2} \dots p_h^{k_h}$. Analogous discussion as above demonstrates that

1) The diagram

$$(10) \quad \begin{array}{ccc} \mathbb{Z}_m^{\mathbb{Z}} & \xrightarrow{T_f} & \mathbb{Z}_m^{\mathbb{Z}} \\ \Phi \downarrow & & \downarrow \Phi \\ \mathbb{Z}_{p_1}^{\mathbb{Z}} \times \cdots \times \mathbb{Z}_{p_h}^{\mathbb{Z}} & \xrightarrow{T_{p_1}^{k_1} \times \cdots \times T_{p_h}^{k_h}} & \mathbb{Z}_{p_1}^{\mathbb{Z}} \times \cdots \times \mathbb{Z}_{p_h}^{\mathbb{Z}} \end{array}$$

is commutative.

- 2) $\Phi := \Phi_{p_1}^{k_1} \times \cdots \times \Phi_{p_h}^{k_h}$ is an isomorphism, and $\mu \cong \mu_{p_1}^{k_1} \times \cdots \times \mu_{p_h}^{k_h}$.
- 3) For any two measurable sets $U, V \in \mathbb{Z}_m^{\mathbb{Z}}$ such that

$$\mu_s(\Phi_s(U) \cap \Phi_s(V)) = \mu_s(\Phi_s(U)) \cdot \mu_s(\Phi_s(V)), \quad s = p_i^{k_i}, 1 \leq i \leq h,$$

then

$$\mu(U \cap V) = \mu(U) \cdot \mu(V).$$

In other words, we have demonstrated the following lemma.

Lemma 4.4. *Suppose $m = p_1^{k_1} p_2^{k_2} \cdots p_h^{k_h}$ for some prime number p_1, \dots, p_h and $k_1, \dots, k_h \in \mathbb{N}$. A linear cellular automaton T_f is strong mixing if and only if $T_{p_i}^{k_i}$ is strong mixing for $1 \leq i \leq h$.*

Proof. Obviously, the strong mixing property of T_f implies $T_{p_i}^{k_i}$ is strong mixing for $1 \leq i \leq h$. Suppose $T_{p_i}^{k_i}$ is strong mixing for $1 \leq i \leq h$. Given two cylinders U and V , let K_i be a positive integer, as indicated in the proof of Lemma 4.2, such that $\mu_{p_i}^{k_i}(T_{p_i}^{-n} U \cap V) = \mu_{p_i}^{k_i}(U) \mu_{p_i}^{k_i}(V)$ for $n \geq K_i$, where $1 \leq i \leq h$. Let $K = \max\{K_i\}$. A straightforward examination infers that

$$\mu(T_f^{-n} U \cap V) = \mu(U) \mu(V) \quad \text{for } n \geq K.$$

This completes the proof. \square

Notably Lemma 4.4 remains true if one replaces strong mixing by either weak mixing or ergodic. The elucidation can be done via a minor modification of the discussion above and is omitted.

As a conclusion of this section, it is seen that Theorem 2.3 follows from Lemmas 4.2 and 4.4.

5. PROOF OF THEOREM 2.5

This section focuses on the proof of Theorem 2.5. Similar to the discussion in Section 4, where the key ideas of the present elucidation are addressed in, it is not difficult to demonstrate that T_f is not a Bernoulli automorphism if there exists a prime factor p of m such that $j_p = 0$. Hence it remains to show that $j_p \neq 0$ for all prime factors p of m implies T_f is a Bernoulli automorphism.

Alternatively, an automorphism T_f is Bernoulli if and only if there is a generator ξ which is Bernoulli for T_f [18]. Let $\xi_{n_1}^{n_2}$ denote the partition consists of all cylinders of the form $[U]_{n_1}^{n_2}$ for $n_1, n_2 \in \mathbb{Z}$. It follows immediately from (5), (7), and the proof of Lemma 4.2 that $\xi_{n_1}^{n_2}$ is a generator provided $n_2 - n_1 \geq r - l$.

Notably, Lemma 4.4 infers that we may assume $m = p^k$ for some prime number p and $k \in \mathbb{N}$ without loss of generality. Moreover, we assume that $r \geq l \geq 0$ for the clarification of the elucidation.

Set ℓ as the smallest positive integer satisfying $2\ell \geq r - l$. Then $\xi_{-\ell}^\ell$ is a generator. Write $\xi_{-\ell}^\ell = \{U_i\}_{i=1}^{m^{2\ell+1}}$. Claim 4.3, which demonstrates that $T_f^{-n}U_i$ is a cylinder for $1 \leq i \leq m^{2\ell+1}$ and $n \in \mathbb{Z}$, together with equations (5), (6), and (7) shows that

$$(11) \quad \bigvee_{i=-n}^0 T_f^i \xi_{-\ell}^\ell \subseteq \xi_{-\ell}^{\ell+nj_p}, \quad \bigvee_{i=N}^{N+n} T_f^i \xi_{-\ell}^\ell \subseteq \xi_{-\ell-(N+n)j_p}^{\ell-Nj_p},$$

if $n = cp^{k-1}$ for some $c \in \mathbb{N}$, and

$$(12) \quad \bigvee_{i=-n}^0 T_f^i \xi_{-\ell}^\ell \subseteq \xi_{-\ell}^{\ell+(cp^{k-1}+1)j_p+d(k-1)(r-j_p)},$$

$$(13) \quad \bigvee_{i=N}^{N+n} T_f^i \xi_{-\ell}^\ell \subseteq \xi_{-\ell-(cp^{k-1}+1)j_p-d(k-1)(r-j_p)}^{\ell-Nj_p},$$

if $n = cp^{k-1} + d$ for some $c \in \mathbb{N}, 1 \leq d < p^{k-1}$, herein

$$N = tp^{k-1} \quad \text{and} \quad t = \max \left\{ 1, \left\lceil \frac{2\ell}{p^{k-1}j_p} \right\rceil \right\}.$$

Notably, both $\bigvee_{i=-n}^0 T_f^i \xi_{-\ell}^\ell$ and $\bigvee_{i=N}^{N+n} T_f^i \xi_{-\ell}^\ell$ are collection of cylinders of the form $[U]_{n_1}^{n_2}$ and $[V]_{n'_1}^{n'_2}$, respectively, where the indices n_1, n_2, n'_1 , and n'_2 , depend on the value of n , are addressed in (11), (12), (13). Analogous discussion as addressed in the proof of Lemma 4.2 indicates that $\bigvee_{i=-n}^0 T_f^i \xi_{-\ell}^\ell$ and $\bigvee_{i=N}^{N+n} T_f^i \xi_{-\ell}^\ell$ are independent. Hence T_f is an Bernoulli automorphism, and this completes the proof of Theorem 2.5.

6. CONCLUSION AND DISCUSSION

This paper investigates invertible linear cellular automata over $\mathbb{Z}_m^{\mathbb{Z}}$ with local rules of the form

$$f(x_l, \dots, x_r) = \sum_{i=l}^r \lambda_i x_i \pmod{m}, \quad l, r \in \mathbb{Z}, m \geq 2.$$

Without using the natural extension, Theorems 2.3 and 2.5 reveal that an invertible linear cellular automaton is strong mixing and is a Bernoulli automorphism with respect to the uniform Bernoulli measure if and only if the canonical projection f_p of f is not permutative at the index $j = 0$ for every prime factor p of m . This gives an affirmative answer for the open problem proposed by Pivato for reversible linear cellular automata [20]. Furthermore, the elucidation extends the results in [14, 25] to all linear automorphisms.

Notably, it can be verified without difficulty that an invertible linear cellular automaton is not ergodic if and only if $j_p = 0$ for some prime factor p of m (cf. Corollary 2.4 and Example 3.3).

Remark 6.1. Notably, one of the key points in demonstrating Theorem 2.3 is that the uniform Bernoulli measure μ is isomorphic to the product measure of those push-forward measures $\mu_{p_1}^{k_1} \times \dots \times \mu_{p_h}^{k_h}$ under canonical projection maps. Hence Theorem 2.3 (resp. Theorem 2.5) remains true for every T_f -invariant measure μ which is isomorphic to the product measure $\mu_{p_1}^{k_1} \times \dots \times \mu_{p_h}^{k_h}$ provided $T_{p_i}^{k_i}$ is strong mixing (resp. Bernoulli) for $T_{p_i}^{k_i}$ -invariant measure $\mu_{p_i}^{k_i}$ for $1 \leq i \leq h$.

The methodology addressed in this paper can be applied to investigating multidimensional reversible linear cellular automata over \mathbb{Z}_m . Meanwhile, the elucidation of ergodic properties of nonlinear cases and cellular automata defined on Cayley graph are in preparation.

REFERENCES

1. H. Akin, J.-C. Ban, and C.-H. Chang, *On the qualitative behavior of linear cellular automata*, J. Cell. Autom. **8** (2013), 205–231, accepted.
2. F. Blanchard, P. Kurka, and A. Maass, *Topological and measure-theoretic properties of one-dimensional cellular automata*, Phys. D **103** (1997), 86–99.
3. F. Blanchard and A. Maass, *Dynamical properties of expansive onesided cellular automata*, Israel J. Math. **99** (1997), 149–174.
4. M. Boyle and A. Maass, *Expansive invertible onesided cellular automata*, J. Math. Soc. Jpn. **52** (2000), 725–740, Erratum, J. Math. Soc. Jpn. **56**, 309310 (2004).
5. G. Cattaneo, A. Dennunzio, and L. Margara, *Solution of some conjectures about topological properties of linear cellular automata*, Theoret. Comput. Sci. **325** (2004), 249–271.
6. G. Cattaneo, E. Formenti, G. Manzini, and L. Margara, *Ergodicity, transitivity, and regularity for linear cellular automata over \mathbb{Z}_m* , Theoret. Comput. Sci. **233** (2000), 147–164.
7. E. M. Coven and M. Paul, *Endomorphisms of irreducible shifts of finite type*, Math. Syst. Theory **8** (1974), 165–177.
8. P. Favati, G. Lotti, and L. Margara, *Additive one-dimensional cellular automata are chaotic according to devaney’s definition of chaos*, Theor. Comput. Sci. **174** (1997), 157–170.
9. G. A. Hedlund, *Endomorphisms and automorphisms of full shift dynamical system*, Math. Systems Theory **3** (1969), 320–375.

10. B. Host, A. Maass, and S. Martínez, *Uniform bernoulli measure in dynamics of permutative cellular automata with algebraic local rules*, Discrete and Continuous Dynam. Systems **9** (2003), 1423–1446.
11. M. Ito, N. Osato, and M. Nasu, *Linear cellular automata over \mathbb{Z}_m* , J. Comput. System Sci. **27** (1983), 125–140.
12. C. Jadur, M. Nasu, and J. Yazlle, *Permutation cellular automata*, Acta Appl. Math. **126** (2013), 203–243.
13. C. Jadur and J. Yazlle, *On the dynamics of cellular automata induced from a prefix code*, Adv. in Appl. Math. **38** (2007), 2753.
14. R. Kleveland, *Mixing properties of one-dimensional cellular automata*, Proc. Amer. Math. Soc. **125** (1997), 1755–1766.
15. G. Manzini and L. Margara, *Invertible linear cellular automata over \mathbb{Z}_m : Algorithmic and dynamical aspects*, J. Comput. System Sci. **56** (1998), 60–97.
16. O. Martin, A. M. Odlyzko, and S. Wolfram, *Algebraic properties of cellular automata*, Commun. Math. Phys. **93** (1984), 219–258.
17. M. Nasu, *The dynamics of expansive invertible onesided cellular automata*, Trans. Am. Math. Soc. **354** (2002), 4067–4084.
18. K. Peterson, *Ergodic theory*, Cambridge University Press, 1990.
19. M. Pivato, *Invariant measures for biperemutative cellular automata*, Discrete and Continuous Dynam. Systems **12** (2005), 723–736.
20. ———, *Ergodic theory of cellular automata*, Encyclopedia of Complexity and Systems Science, Springer New York, 2009, pp. 2980–3015.
21. M. Pivato and R. Yassawi, *Limit measures for affine cellular automata*, Ergodic Theory Dynam. Systems **22** (2002), 1269–1287.
22. ———, *Limit measures for affine cellular automata II*, Ergodic Theory Dynam. Systems **24** (2004), 1961–1980.
23. M. Sablik, *Measure rigidity for algebraic bipermutative cellular automata*, Ergodic Theory Dynam. Systems **27** (2007), 1965–1990.

- 24. ———, *Directional dynamics for cellular automata: A sensitivity to initial conditions approach*, Theoret. Comput. Sci. **400** (2008), 1–18.
- 25. M. A. Shereshevsky, *Ergodic properties of certain surjective cellular automata*, Monatsh. Math. **114** (1992), 305–316.
- 26. M.A. Shereshevsky, *K-property of permutative cellular automata*, Indag. Math. (N.S.) **8** (1997), 411–416.

DEPARTMENT OF APPLIED MATHEMATICS, NATIONAL UNIVERSITY OF KAOHSIUNG,
KAOHSIUNG 81148, TAIWAN, ROC.

E-mail address: `chchang@nuk.edu.tw`; `hchang@nuk.edu.tw`